NISTTech

K-ZERO DAY SAFETY

Docket No. 12-017, Publication No. US 2012-0233699

Abstract

The security risk of a network against unknown zero day attacks has been considered as something unmeasurable since software flaws are less predictable than hardware faults and the process of finding such flaws and developing exploits seems to be chaotic. In this paper, we propose a novel security metric, k-zero- day safety, based on the number of unknown zero day vulnerablities. That is, the metric simply counts how many vulnerabilities would be required for compromising a network asset, regardless of what vulnerabilities those might be. We formally define the metric based on an abstract model of networks and attacks. We then devise algorithms for computing the metric. Finally, we show the metric can quantify many existing practices in hardening a network.

Inventors

- Wang, Lingyu
- Singhal, Anoop
- Jajodia, Sushil

References

- Serial No. 13/348,457, Filed on 1/11/2012, Published on 9/13/2012, Expires on 1/11/2032

Status of Availability

This invention is available for licensing exclusively or non-exclusively in any field of use.

Last Modified: 05/29/2015